BSTZ No. 080398.P252X3
Express Mail No. EV323394255US

UNITED STATES PATENT APPLICATION

FOR

System, Method and Apparatus for Secure Digital Content Transmission

Inventor:
Brant L. Candelore

Prepared by:

Blakely, Sokoloff, Taylor & Zafman LLP
12400 Wilshire Boulevard, Suite 700
Los Angeles, California 90025
(714) 557-3800

SYSTEM, METHOD AND APPARATUS FOR SECURE DIGITAL CONTENT TRANSMISSION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation-in-part of United States Patent Application No. 10/387,163 filed March 11, 2003, which is a continuation-in-part application of United States Patent Application No. 09/497,393 filed February 3, 2000, which is based on a United States Provisional Application No. 60/126,805, filed on March 30, 1999.

BACKGROUND

1. Field

[0002] Embodiments of the invention relate to content protection. More specifically, one embodiment of the invention relates to an apparatus and method for enabling the exchange of information in a secured manner in order to protect digital content being transmitted.

2. General Background

[0003] Analog communication systems are rapidly giving way to their digital counterparts. Digital television is currently scheduled to be available nationally. High-definition television (HDTV) broadcasts have already begun in most major cities on a limited basis. Similarly, the explosive growth of the Internet and the World Wide Web have resulted in a correlative growth in the increase of downloadable audio-visual files, such as MP3-formatted audio files, as well as other content.

[0004] Simultaneously with, and in part due to this rapid move to digital communications system, there have been significant advances in digital recording devices.

Digital versatile disk (DVD) recorders, digital VHS video cassette recorders (D-VHS VCR), CD-ROM recorders (e.g., CD-R and CD-RW), MP3 recording devices, and hard disk-based recording units are but merely representative of the digital recording devices that are capable of producing high quality recordings and copies thereof, without the generational degradation (i.e., increased degradation between successive copies) known in the analog counterparts. The combination of movement towards digital communication systems and digital recording devices poses a concern to content providers such as the motion picture and music industries, who desire to prevent the unauthorized and uncontrolled copying of copyrighted, or otherwise protected, material.

[0005] In response, there is a movement to require service providers, such as terrestrial broadcast, cable and direct broadcast satellite (DBS) companies, and companies having Internet sites which provide downloadable content, to introduce protection schemes. It is noted that one of the currently proposed schemes involve symmetric key cryptographic techniques to encode components of a compliant device. This allows for the authentication of any digital device prior to transmission of the digital content in order to determine whether the device is compliant.

[0006] However, this scheme fails to provide a technique that has universal application and does not impose rigorous key management as normally associated with symmetric key-based systems.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Embodiments of the invention are illustrated by way of example and not by way of limitation in the figures of the accompanying drawings, in which like references indicate similar elements and in which:

[0008] Figure 1 is a first exemplary embodiment of a secure content delivery system;

[0009] Figure 2 is a second exemplary embodiment of a secure content delivery system;

[0010] Figures 3 and 4 are exemplary embodiments of methods for encrypting and decrypting a control word;

[0011] Figure 5 is a more detailed illustration of the decoder adapted to the headend of Figure 2;

[0012] Figure 6 is an exemplary embodiment of services that may be delivered to the decoder of Figure 2;

[0013] Figure 7 is a third exemplary embodiment of a secure content delivery system;

[0014] Figure 8 is an exemplary embodiment of the mating key gateway in communications between the headend and a source of the mating keys;

[0015] Figure 9A a first exemplary embodiment of a mating key lookup table stored within the storage unit of Figure 8;

[0016] Figure 9B a second exemplary embodiment of a mating key lookup table stored within the storage unit of Figure 8;

[0017] Figure 9C a third exemplary embodiment of a mating key lookup table stored within the storage unit 560 of Figure 8;

[0018] Figure 10 is an exemplary embodiment of a data structure forming the mating key generator transmitted through a secure content delivery system;

[0019] Figure 11 is an exemplary embodiment of an entitlement management message (EMM) routed to a digital device from the headend;

[0020] Figure 12 is a fourth exemplary embodiment of a secure content delivery system;

[0021] Figure 13 is an exemplary embodiment of meta-data associated with an electronic program guide (EPG) routed to a digital device;

[0022] Figure 14 is a first exemplary embodiment of the descrambler IC adapted for implementation within a decoder of the digital devices set forth in the systems of Figures 2, 7,and 12;

[0023] Figure 15 is a second exemplary embodiment of the descrambler IC adapted for implementation within a decoder of the digital devices set forth in the systems of Figures 2, 7,and 12; and

[0024] Figure 16 is a portion of a fifth exemplary embodiment of a secure content delivery system.

DETAILED DESCRIPTION

[0025] Various embodiments of the invention relate to an apparatus, system and method for protecting the transfer of data. In one embodiment, such protection involves the descrambling or decrypting of digital content from one or more service providers in digital devices. Examples of a "service provider" include, but are not limited to a terrestrial broadcaster, cable operator, direct broadcast satellite (DBS) company, a company providing content for download via the Internet, or any similar sources of content.

[0026] A "trusted third party" is an entity that is responsible for ensuring that information is protected and accurately distributed. It is contemplated that the trusted third party may be selected so as to have no affiliation with one of the content providers, service providers or the digital device manufacturers. Examples of trusted third parties may include, but is not limited or restricted to a governmental entity, financial institution, an independent security entity (e.g., Verisign of Mountain View, California) or the like.

[0027] In the following description, certain terminology is used to describe features of the invention. For example, the terms "component", "block" or "logic" are representative of hardware and/or software configured to perform one or more functions. For instance, examples of "hardware" include, but are not limited or restricted to an integrated circuit such as a processor (e.g., microprocessor, application specific integrated circuit, a digital signal processor, a micro-controller, etc.). Of course, the hardware may be alternatively implemented as a finite state machine or even combinatorial logic.

[0028] An example of "software" includes executable code in the form of an application, an applet, a routine or even a

collection of instructions. The software may be stored in any type of machine readable medium such as a programmable electronic circuit, a semiconductor memory device such as volatile memory (e.g., random access memory, etc.) and/or non-volatile memory (e.g., any type of read-only memory "ROM", flash memory), a floppy diskette, an optical disk (e.g., compact disk or digital video disc "DVD"), a hard drive disk, tape, or the like.

[0029] The term "program data" generally represents any type of information being transferred over a secure content delivery system. Examples of program data include system information, one or more entitlement control messages or entitlement management messages, digital content, and/or other data, each of which will be described briefly below. A "message" is a collection of bits sent as a bit stream, a packet or successive packets.

[0030] The term "transmission medium" generally represents a communication pathway between two devices. Examples of transmission medium include, but are not limited to electrical wire, optical fiber, cable, a wireless link established by wireless signaling circuitry, or the like.

[0031] Referring to Figure 1, a first exemplary embodiment of a secure content delivery system 10 that comprises an entertainment system 100 is shown. Herein, the secure content delivery system 10 comprises a headend 20 that communicates with a mating key gateway 30 over a transmission medium 40. The headend 20 receives one or more mating keys from mating key gateway 30. These mating keys may be used to encrypt a program key, which is defined as information used to encrypt digital content. Examples of a program key include, but are not limited or restricted to one or more control words, one or more service keys, one or more precursor keys, or one or more keys used to derive a control word, service key or precursor key. The headend 20 encrypts the digital

content before transmission to the entertainment system 100 via a transmission medium 50. The mating keys may be transmitted along with the digital content or are recreated at the entertainment system 100.

[0032] The entertainment system 100 comprises a digital device 110 for receiving information including program data from one or more service providers. The program data may be propagated as a digital bit stream for example. The digital device 110 may be implemented in a wide range of configurations, such as a set-top box, television, computer, audio-playback device (e.g., digital radio), audio-recording device (e.g., MP3 player), video-recording device (e.g., TIVO® recorder by TiVo Inc. of Alviso, California), or the like.

[0033] For instance, the digital device 110 may be configured in accordance with an embedded security architecture, a split security architecture, or an external security architecture. As an embedded architecture, in one embodiment, digital device 110 is implemented as a set-top box that comprises fixed, internal circuitry supporting both entitlement management and descrambling operations.

[0034] Alternatively, in accordance with a split security architecture embodiment, the digital device 110 may be adapted to receive a removable smart card that handles entitlement management, while descrambling of incoming program data is controlled by internal circuitry.

[0035] Yet, in accordance with an external security embodiment, the digital device 110 may be a "point-of-deployment" product, e.g. called CableCARD in U.S. cable, with a PCMCIA form factor card handling both entitlement management and descrambling operations by sending and receiving messages over either an In-Band channel or an Out-of-Band channel.

[0036] Of course, as yet another alternative embodiment, external security type may also be split so that the PCMCIA card may be configured to handle descrambling operations, but adapted to communicate with a smart card for handling entitlement management. These and other embodiments of the digital device 110 may be implemented while still falling within the spirit and scope of the invention.

[0037] The digital device 110 comprises a receiver 111, which processes the incoming program data and places digital content in a perceivable format (e.g., viewable and/or audible). The receiver 111 may be configured as a decoder as described below. As mentioned previously, the program data may include at least one or more of the following: system information, entitlement control messages, entitlement management messages and digital content.

[0038] Herein, "system information" may include information on program names, time of broadcast, source, and a method of retrieval and decoding, and well as copy management commands that provide digital receivers and other devices with information that will control how and when program data may be replayed, retransmitted and/or recorded. These copy management commands may also be transmitted along with an entitlement control message (ECM), which is generally used to regulate access to a particular channel or service.

[0039] An "Entitlement Management Message" (EMM) may be used to deliver entitlements (sometimes referred to as "privileges") to the digital receiver 111. Examples of certain entitlements may include, but are not limited to access rights, access parameters, and/or descrambling keys. A descrambling key is generally a code that is required by descrambler logic to recover data in the clear from a scrambled format based on the entitlements granted.

Finally, "content" in the program data stream may include images, audio, video or any combination thereof. The content may be in a scrambled or clear format.

[0040] As shown, the digital device 110 may be coupled to other components in the entertainment system 100 via a transmission medium 120. The transmission medium 120 operates to transmit control information and data, such as a portion of the program data for example, between the digital device 110 and other components in the entertainment system 100.

[0041] Depending on the type of product corresponding to the digital device 110, the entertainment system 100 may comprise an audio system 130 coupled to the transmission medium 120. A digital VCR 140, such as a D-VHS VCR, may also be coupled to the digital device 110 and other components of the entertainment system 100 through the transmission medium 120.

[0042] A hard disk recording unit 150 may also be coupled to digital device 110 and other components via transmission medium 120. Display 160 may include a high definition television display, a monitor or another device capable of processing digital video signals, or a monitor capable of processing analog video signals after digital-to-analog conversion. Finally, a control unit 170 may be coupled to the transmission medium 120. The control unit 170 may be used to coordinate and control the operation of some or each of the components on the entertainment system 100.

[0043] The content of a digital program may be transmitted in scrambled form. In one embodiment, as part of the program data, access requirements may be transmitted along with the scrambled content to the digital device 110 that is implemented with the receiver 111 functioning as a conditional access unit, especially when the digital device 110 operates as a set-top box. An "access requirement" is a restrictive parameter used to determine if the digital device 110 implemented with conditional

access functionality is authorized to descramble the scrambled content for viewing or listening purposes. For example, the access requirement may be a key needed to perceive (view and/or listen to) the content, a service tag associated with a given service provider, or even a particular descrambling software code.

[0044] When a scrambled program is received by the digital device 110, the access requirements for the program are compared to the entitlements that the digital device 110 actually has. In order for the digital device 110 to display the scrambled content in clear form, in one embodiment, the access requirements for the program are compared to the entitlements of the digital device 110. The entitlements may state that the digital device 110 is entitled to view/playback content from a given content provider such as Home Box Office (HBO), for example. The entitlements may also include one or more keys needed to descramble the content. The entitlements also may define the time periods for which the digital device 110 may descramble the content.

[0045] Thus, in one embodiment, access requirements and entitlements form a part of the access control system to determine whether a user is authorized to view a particular program. It is contemplated that the description below focuses on mechanisms to recover audio/visual content such as television broadcasts, purchased movies and the like. However, it is contemplated that the invention is also applicable to the descrambling of audible content only (e.g., digitized music files).

[0046] The access requirements may be delivered to the digital device 110 using Entitlement Control Messages (ECMs)delivered in packets with different packet identifiers (PIDs). Each packet with the corresponding PID may contain the access requirements associated with a given service or feature. The content that is delivered

to the digital device 110 may also include packet with a large number of different PIDs, thus enabling special revenue features, technical features, or other special features to be performed locally.

[0047] Referring now to Figure 2, a second exemplary embodiment of a secure content delivery system 200 that comprises a decoder 220 adapted for communications with a headend 210 is shown. For this embodiment, the decoder 220 comprises an interface 225, an optional processor 230, an optional memory 235, a descrambler integrated circuit (IC) 240 and a descrambler unit 270.

[0048] In communication over a one-way or two-way network 215, headend 210 maintains the access rights for a digital device operating as the decoder 220. The headend 210 can deliver one or more encrypted program keys to the decoder 220 (hereinafter generally referred to as an "encrypted key"). Produced by encryption block 214, the encrypted key is based on information stored in memory 212. This information is equivalent to or a derivation of at least one unique key (referred to as "Unique Key") stored in a memory 250 of the descrambler IC 240.

[0049] In accordance with one embodiment of the invention, the encrypted key may be stored locally within the memory 235 to facilitate transitions from one channel to another. However, in accordance with other embodiments of the invention, the encrypted key may be stored in memory 250 of the descrambler IC 240 or loaded as needed from the headend 210 into the descrambler IC 240 and decrypted only by decryption block 260 in the descrambler IC 240 using the Unique Key stored in memory 250.

[0050] In one embodiment, the program key is a control word which is supplied to the descrambler unit 270 to descramble the content directly. In another embodiment, the program key is a service key used to decrypt one or more control words, which are received in-band with the

scrambled content and subsequently used by the descrambler unit 270 for descrambling purposes.

[0051] Embodiments of the encryption and decryption functions performed by encryption block 214 and decryption block 260 are shown in Figures 3 and 4. These operations transform the program key based on the Unique Key (or derivations thereof) stored in memories 212 and 250. Any encryption algorithm may be used such as DES, M6, DVB Common Scrambling Algorithm (CSA), Advanced Encryption Standard (AES) or Triple DES (3DES) as shown.

[0052] Referring back to Figure 2, the descrambler IC 240 may use AES or 3DES to decrypt the key in decryption block 260. The decrypted program key is then used by descrambler unit 270 to descramble the scrambled content 280 and output clear content 290. It is contemplated that the algorithm used to encrypt and decrypt the key may be different than the algorithm used to scramble and descramble the content. These different proprietary algorithms may be considered as anti-piracy measures to invalidate clone hardware.

[0053] Since the encryption and decryption of the program key is local to the digital device, it is possible to phase in the deployment of increasingly more robust encryption. For example, single DES may be initially deployed, and later double or 3DES can be phased in with no consequence to already fielded paired units of digital devices. The key length of the Unique Key 250 may be at least as large as the decrypted key, to help reduce attacks on the Unique Key by hackers.

[0054] The headend 210 can deliver one or more program keys on a channel or "tier of service" basis in EMMs. The program keys are encrypted, stored locally in decoder 220 and used by a processor 230 as needed when tuning to different channels. Because the digital devices may be fielded in high volume as compared to the headend 210, eliminating the smart cards (and corresponding

cryptographic processors), from the digital devices greatly reduces the cost of implementing a pay-TV system in a network.

[0055] While this embodiment works in one-way (non-IPPV) broadcast networks, it also performs in two-way, interactive networks, where the program keys for a particular service are requested, such as IPPV or VOD purchases or any other non-subscription service. As shown, a return communication path 221 is used to request the key because the ability to grant access to a new service is performed by the headend 210 instead of a local controlling cryptographic processor.

[0056] In order to avoid overload problems at the headend 210 caused by a large number of simultaneous impulse buys of IPPV programs, a Free Preview period can be determined and IPPV programs can be marketed in advance of the actual viewing. In this embodiment, program keys (e.g., service keys) for individual shows or movies may be requested by the decoder 220 and delivered ahead of time. For example, interactive networks, such as a cable system having the return communication path 221, which is in-band (IB) or out-of-band (OOB) such as via a DOCSIS modem or Out-of-Band transmitter/receiver for example, can deliver a Request for Program Key (RPK) message from the decoder 220 to the headend 210. Alternatively, the decoder 220 may request the program keys in real-time for each program accessed.

[0057] A controller (not shown) at the headend 210 processes the RPK message. The RPK message may contain an address of the decoder 220 as well as information needed to identify the channel to be viewed. The RPK message may be encrypted, if desired, for non-repudiation and prevention of denial of service attacks, such as IPPV or VOD requests for example.

[0058] Upon receipt of the RPK message, the headend 210 accesses entries of an access control list (listing each

entitlement of the decoder 220) and verifies the decoder is authorization to receive a particular program key (e.g., service key). If authorized, the headend server 210 sends the program key (encrypted using a key identical to or a derivative of the Unique Key 250) to the decoder 220.

[0059] Figure 5 provides a more detailed illustration of the decoder 220 of Figure 2 adapted to the headend 210 for request and receipt of one or more program keys (e.g., service keys). According to one embodiment, program data 300 such as an Entitlement Control Message (ECM) or meta-data associated with an Electronic Program Guide (EPG) as well as scrambled content is provided to the decoder 220 by a service provider. The program data 300 includes scrambled content as well as conveys at least an identifier of the desired channel or service (referred to as "Channel or Service ID"). In the event that the program data 300 is an IPPV or VOD program, the program data 300 may further include a Program identifier (PID). This is because no ECM processing other than identifying the appropriate encrypted key from memory, and using it to write it into the appropriate storage element (or register) of the descrambler IC 240 needs to be performed.

[0060] An MPEG Demultiplexer 310 operates as a message processor to extract the Channel or Service ID upon detection in program data. The Channel or Service ID are routed to the processor 230 which, in combination with transmitter/receiver logic 320, generates a Request for Program Key (RPK) message for transmission to the headend 210 over communication path 221.

[0061] In response, upon authorization of the decoder 220, the headend 210 transmits the requested program key (PK) in an encrypted format to the transmitter/receiver logic 320, which provides the encrypted PK to the processor 230. The processor 230 may store the encrypted PK in the memory 235 and/or provide the encrypted PK to the descrambler IC

240 for descrambling incoming scrambled content in real-time. The decrypted PK may be used to decrypt an entitlement control message (ECM) sent in-band which could be decrypted in subsequent steps in the descrambler IC 240. But, an ECM is not necessary. The memory 235 is an optional component for use if it is desirable to store the encrypted PK locally. Where the encrypted PK is not stored locally but is accessed from the headend 210 as needed, the memory 235 may be removed from the decoder 220.

[0062] Upon receiving the scrambled content of the program data, the descrambler IC 240 descrambles such content, which is subsequently supplied to the MPEG decoder 330 if the content is compressed with a MPEG format. The MPEG decoder 330 decompresses the digital content and subsequently routes the decompressed digital content to either a digital-to-analog (D/A) converter for display on a television, a Digital Video Interface (DVI) link or a network interface (e.g., IEEE 1394 link).

[0063] As shown, the processor 230, memory 235, descrambler IC 240, MPEG demultiplexer 310, transmitter/receiver logic 320 and MPEG decoder 330 may be implemented on two or more integrated circuits interconnected through bus traces or another communication scheme (e.g., wires, optical fiber, etc.). Alternatively, these components may be implemented on a single integrated circuit.

[0064] In this embodiment, the PK may be valid for a certain period of time. The decoder 220 may store the PK in the memory 235, allowing the decoder 220 to re-access the service when PK is still valid. In this embodiment, the PK is stored in encrypted form (as it comes over the network from the headend 210) in the memory 235.

[0065] The PK may be valid for the duration of a program or it may be valid for a selected period of time, e.g. six hours. Using a key for a longer period of time will reduce the overall number of transactions between the

decoder 220 and the headend 210 because, once the key is stored in the memory 235 of the decoder 220, it is readily available. Depending on the duration of the current program key (e.g., PK), the next Program Key (PK_{next}) may be delivered along with the PK, both may be in encrypted format. Alternatively, the decoder 220 may request the PK_{next} after detecting the end of the PK's valid epoch (e.g., time duration of the PK). In one embodiment, the program key is valid for the duration of a user's subscription period.

[0066] The program key should be identified properly so that it may be applied to a channel being tuned to. According to one embodiment, when the decoder 220 tunes to a channel, it looks up the appropriate encrypted program key from the memory 235 and writes that into the Odd/Even MPEG key register of the descrambler IC 240. As in the embodiment of Figure 2, the secret Unique Key information may be programmed into the descrambler IC 240 when decoder 220 is manufactured.

[0067] In one embodiment, one type of program key, namely a service key, may comprise 56-bit, 112-bit, or 168-bit keys. Table 1 shows the storage requirements for different sizes of keys.

Table 1: Number of Bytes to Store Independent Service Keys

Number of Channels with Independent Keys	Channel ID (3 Bytes)	16 Byte Triple DES Encrypted Service Key	16 Byte Triple DES Encrypted Service Key	Total Bytes
		CURRENT	NEXT	
20	60	320	320	700
50	150	800	800	1,750
100	300	1600	1600	3,500
200	600	3200	3200	7,000
400	1200	6400	6400	14,000

[0068] Services can be sold a-la-carte or sold as a bouquet or package. There may be several tiers of services, each identified by a Service ID. For example, there may be a basic tier of services 360, a medium tier 370 offering more services, and advanced tiers 370 offering different premium services, as shown in Figure 6. In this embodiment, each incremental tier of services may be given a separate program key.

[0069] From Table 1 above, if a customer where to subscribe to 20 different types of Service tiers, that would require 60 bytes of ID storage, 320 bytes of storage of the currently valid service keys, 320 bytes of storage for the service keys valid for the next epoch (or billing period) for a total of 700 bytes.

[0070] Referring now to Figure 7, a third exemplary embodiment of a secure content delivery system 400 is shown. The secure content delivery system 400 comprises a

headend 405, either a plurality of mating key servers associated with different device manufacturers 430_1-430_N ($N \geq 2$) or a trusted third party 435, a digital device 440 and a mating key gateway 450. Herein, headend 405 comprises a subscriber management system 410 and a Conditional Access (CA) control system 420 as described below.

[0071] Although not shown, it is contemplated that the CA control system 420 could be configured to perform a lookup of databases containing serial numbers of the digital devices, thereby eliminating required implementation of and access to the subscriber management system 410.

[0072] As shown in Figure 8, the mating key gateway 450 comprises a processor 500, a random access memory 510 coupled to the processor 500 via a first bus 520 (a processor bus) and a chipset 530 that couples the first bus 520 to a second bus 540 (e.g., an input/output "I/O" bus). Second bus 540 is coupled to an interface 550 that is adapted to receive signaling from one or more of the following: (1) headend 405, (2) any of the servers 430_1,…, and/or 430_N supported by a supplier (e.g., digital device manufacturer, distributor, etc.), and (3) trusted third party 435. The interface 550 may be a modem, a networking card, or other communication logic that supports communications with a physically distant unit (e.g., headend 405, mating key servers 430_1-430_N, trusted third party 435, etc.). These communications may identify the unit through dynamic or static addresses (e.g., media access control "MAC" addresses, Internet Protocol "IP addresses and the like).

[0073] The second bus 540 also supports a non-volatile (NV) storage unit 560 such as a hard disk drive, an optical drive, an opto-electric device (e.g., compact disk player, digital versatile disk "DVD" player, etc.). NV storage unit 560 is configured to store a mating key lookup table as described in Figures 9A-9C.

[0074] Referring now to Figure 9A, a first exemplary embodiment of a mating key lookup table stored within the storage unit 560 of Figure 8 is shown. The storage unit 560 stores a mating key lookup table 570 that features a first group of entries 572 forming a range of serial numbers associated with each digital device supplied by an entity (e.g., manufacturer, distributor, etc.). In addition, the lookup table 570 further comprises a second group of entries 574, each corresponding to one serial number and identifying an address used to establish communications with an appropriate mating key server. For instance, all serial numbers with the most significant byte value equivalent to "00" (grouping 576) designate that at least the mating key generator accompanying the serial number is transmitted to a mating key server associated with or controlled by one of the entities such as Sony Corporation for this embodiment.

[0075] Referring to Figure 9B, in the alternative, the storage unit 560 may be adapted to store a mating key lookup table 580 that features a first group of entries 582 forming a range of mating key generators associated with each digital device provided by a supplier (e.g., manufacturer, distributor, etc.). As described below in Figure 10, each mating key generator comprises an identifier of a supplier, such as a Manufacturer ID for example, which can be used to identify an intended recipient of the mating key generator. A second group of entries 584 is arranged to identify an address for establishing communications with a mating key server associated with or supported by the identified manufacturer. For instance, in response to a selected portion (e.g., first byte) of the mating key generator having a predetermined value, the mating key generator is transmitted to a mating key server associated with or controlled by a predetermined entity (e.g., Sony Corporation as shown).

[0076] Referring now to Figure 9C, as another alternative embodiment, the storage unit 560 may be adapted to store a mating key lookup table 590 that features a first group of entries 592 along with a correspond second group of entries 594. The first group of entries 592 features received mating key generators "MKG" while the second group 594 features one or more mating keys corresponding to the particular mating key generator. The mating key(s) may be received from the trusted third party 435 or at least one of the mating key servers 430_i ($1 \leq i \leq N$) as shown in Figure 7 and described below.

[0077] Referring back to Figure 7, once a user of the digital device 440 desires to receive particular program data, the digital device 440 determines whether entitlements associated with the requested program data are already stored therein. If the entitlements are not stored, the user may be notified by a screen display and prompted to provide a request 411 (e.g., a RPK message over communication path 221) to the headend 405. The request 411 may be provided by the user via (i) an out-of-band (OOB) communication pathway (e.g., electronic mail over the Internet, or telephone call by the user, etc.) to the CA control system 420 in communication with digital device 440 as shown. Alternatively, the request 411 may be sent automatically or may be routed to CA control system 420 of headend 405, which performs a lookup of information to authorize the user substantially in real time.

[0078] For one embodiment, the request 411 is a message that comprises an identifier (e.g., an alphanumeric, or numeric code) of the requested content and a serial number of the digital device (referred to as "Serial Num"). Implemented as any information processing system (e.g., server, relay station or other equipment controlled by a service provider or content provider), the subscriber management

system 410 processes the request 411 and determines what entitlements are to be provided to the digital device 440.

[0079] Upon receiving an authorization (AUTH) message 412 from the subscriber management system 410, which may include the Serial Num 441 and perhaps global keys (e.g., keys used to decrypt ECMs sent in-band with the content), the CA control system 420 routes the Serial Num 441 and a mating key generator 421 to the mating key gateway 450. For one embodiment of the invention, the mating key gateway 450 accesses the Manufacturer ID of the digital device 440 from the mating key generator 421 and appropriately routes the mating key generator 421 and Serial Num 441 to a selected mating key server 430_i.

[0080] Alternatively, it is contemplated that the CA control system 420 may simply route the mating key generator 421 to the mating key gateway 450. The mating key gateway 450 accesses the Manufacturer ID from the mating key generator 421 which comprises a first portion that identifies a selected mating key server 430_i to receive the mating key generator 421 and a second portion that identifies the particular digital device. The mating key server 430_i uses the mating key generator 421 to produce the mating key 422 and returns the mating key 422 to the CA control system 420.

[0081] Alternatively, instead of the mating key gateway 450 routing the mating key generator 421 and optionally the Serial Num 441 to a selected mating key server 430_i, it is contemplated that such information may be routed to the trusted third party 435, which accesses a database for retrieval of a mating key. The mating key is based on values associated with the mating key generator 421 and/or Serial Num 441. Each database may be allocated a range of values where values associated within the mating key generator 421 and/or the Serial Num 441 can be used to identify a targeted database from which the mating key 422 is accessed.

[0082] Prior to transmission of the Serial Num 441 and/or the mating key generator 421, the CA control system 420 may perform an authentication scheme with the mating key gateway 450. Also, authentication schemes may be performed between mating key gateway 450 and either a selected mating key server 430_i or the trusted third party 435. Each authentication schemes produces a session key that is used to encrypt information exchanged between the parties in order to provide a secure link there between. Examples of various types of authentication schemes include an exchange of digital certificates, digital signatures, hash values or the like.

[0083] As shown in Figure 10, the mating key generator 421 is a message that comprises one or more of the following: a identifier of the supplier such as a Manufacturer ID 600, a Service Provider ID 610, a conditional access (CA) Provider ID 620 and a Mating Key Sequence Number 630. For this embodiment, "Manufacturer ID" 600 is a predetermined value that identifies a manufacturer of the digital device 440. Of course, it is contemplated that the Manufacturer ID 600 is optional, depending on the particular arrangement of the Serial Num 441. The "Service Provider ID" 610 is a value (e.g., one or more bits such as 16-bits) that identifies the communications system provider as well as the selected distribution mechanism. For example, the Service Provider ID 610 may identify which cable, satellite, terrestrial or Internet company is supplying the requested program data and/or the particular head-end server of that company.

[0084] The "CA Provider ID" 620 indicates the provider of the CA control system 420. The "Mating Key Sequence Number" 630 is used for aging purposes in order to indicate expiration of the mating key generator 421.

[0085] Referring back to Figure 7, the Serial Num 441 may have a unique portion for each Manufacturer ID 600 in order to identify the mating key server 430_1,..., or 430_N (or

database of trusted third party 435) to which access is sought. Alternatively, the Serial Num 441 may be expanded to include a serial number of the digital device 440 as well as a code field to identify the manufacturer of that digital device 440. Hence, the Manufacturer ID 600 may be excluded from the mating key generator 421. Of course, the number of bits is a design choice.

[0086] Upon receipt of the mating key generator 421 and the Serial Num 441, the appropriate mating key server (e.g., server 430_i, where $i \geq 1$) or trusted third party 435 returns one or more mating keys 422. The mating key 422 may be generated based on computations involving a one-time programmable (OTP) key value some or all of the information supplied by the mating key generator 421. For instance, as previously shown in Figures 2 and 5, the OTP value is identical to the Unique Key stored in internal memory 250 of the descrambler IC 240. At least a portion of information from the mating key generator 421, namely the Manufacturer ID 600, Service Provider ID 610, CA Provider 620, Mating Key Sequence Number 630 of Figure 10 or any combination thereof, undergoes a computation (e.g., encryption, hashing, etc.) with the OTP value to produce the mating key 422. According to one embodiment, the OTP value may be located using the Serial Num 441.

[0087] In one embodiment of the invention, the mating key 422 is used to encrypt a program key (e.g., control word, service key, etc.) needed to descramble scrambled content being sent to the digital device 440. More specifically, according to one embodiment of the invention, the mating key server 430_i accesses a key being an identical copy of Unique Key 250 of Figure 2 and encrypts or decrypts the mating key generator 421 using the accessed key. This produces the mating key 422. Alternatively, it is contemplated that the mating key generator 421 may undergo a one-way hash operation in which the result is encrypted or decrypted, or a portion of the mating key generator 421

encrypted or decrypted in lieu of the entire message 421 being encrypted or decrypted.

[0088] Upon receipt of the mating key 422, the CA control system 420 generates an entitlement management message (EMM) 460 along with one or more ECMs 470. One embodiment of EMM 460 is illustrated in Figure 11. Moreover, as an optional function, the CA control system 420 may produce derivative keys of the mating key 422. These derivative keys are used to encrypt a corresponding number of program keys, which after encryption, are sent to the digital device 440 for subsequent descrambling operations.

[0089] As shown in Figure 11, EMM 460 comprises at least two of the following: Serial Num 441, EMM length field 700, mating key generator 421, "M" ($M \geq 1$) key identifiers 710_1-710_M and encrypted service keys 720_1-720_M associated with the key identifiers 710_1-710_M, respectively. Of course, the size (in bits) of these values can be varied and other types of entitlements 730 besides identifiers or service keys may be included in the EMM 460. Also, it is contemplated that the mating key generator 421 may be excluded from the EMM 460 and sent separately and generally concurrent with the EMM 460. Of course, the size (in bits) of these values/fields can be varied.

[0090] The Serial Num 441 is a value that is used to indicate a particular digital device and perhaps the manufacturer of the set-top box. It may be the identification of the smart card (if used), or public identification number of the descrambler IC 240. The "EMM length field" 700 is a bit value that is used to indicate the length of the EMM 460. The mating key generator 421, as shown, is a bit value that includes the parameters forth above in Figure 10. Each "key identifier" 710_1-7104_M is a 16-bit value that indicates a tier of service associated with a corresponding encrypted service key 720_1-720_M, respectively. The encrypted service keys 720_1-720_M are decrypted by a key produced within the descrambler IC

240 that is identical to the mating key 422 as shown in Figure 7.

[0091] Figure 12 is a fourth exemplary embodiment of a secure content delivery system 800. The secure content delivery system 800 comprises a subscriber management system 810 and a CA control system 820, a plurality of mating key servers 830_1-830_N and/or trusted third party 835, a digital device 840, a mating key gateway 850 (similar to gateway 450 of Figure 7), and a network interface 860 (e.g., DOCSIS CMTS). The digital device 840 comprises a descrambler IC 860 including local memory 870 configured to store a unique key 880 of the digital device 840.

[0092] The digital device 840 receives electronic program guide (EPG) meta-data with the EPG in an unscrambled format and digital content 848 in a scrambled format. According to one embodiment of the invention, the EPG meta-data 900 is provided out-of-band by CA control system 820. It is contemplated, however, that the EPG meta-data 900 may be provided in-band. The EPG meta-data 900 may preclude the need to send ECMs in-band. If ECMs are sent, then they can deliver faster changing keys which can be processed in multiple iterations in decryption block 260.

[0093] As shown in Figure 13, one embodiment of the EPG meta-data 900 includes multiple tag entries 910_1-910_S ($S \geq 1$) for different types of content provided by a service provider. Each tag entry (e.g., tag entry 910_j) comprises at least a channel name 920_1, a name of the content 930_1, and a key identifier 940_1 indicating the tier of service associated with the channel. In addition, each tag entry 910_1 further comprises a program identifier (PID) 950_1 and a mating key generator (MKG) 960_1.

[0094] Referring back to Figure 12, once a user of the digital device 840 desires to receive particular type of content (e.g., PPV movie, broadcast channel, etc.), the digital device 840 determines whether entitlements

associated with the requested content are already stored therein. If the entitlements are not stored, the user may be either (1) notified directly through a screen display or audio playback and prompted to provide a request 811 to the subscriber management system 810 (or CA control system 820) or (2) the request 811 may be sent automatically. The request 811 may be provided out-of-band (e.g., telephone call or e-mail over Internet) or in-band (depression of order button on remote for transmission to subscriber management system 810 via CA control system 820).

[0095] Herein, the request 811 may be a message (e.g., RPK message) that comprises a serial number of the set-top box (referred to as "Serial Num") and an identifier (e.g., an alphanumeric or numeric code) of the requested content. The subscriber management system 810 processes the request 811 and determines what entitlements are to be provided to the digital device 840.

[0096] Upon receiving an authorization (AUTH) message 812 from the subscriber management system 810, including the Serial Num 841, information for constructing a mating key generator 821, and entitlements for constructing an EMM, the CA control system 820 routes the Serial Num 841 and the mating key generator 821 to the mating key gateway 850. The mating key gateway 850 operates as an intermediary to coordinate delivery of a mating key 822 that is used to extract the requested content from downloaded, scrambled information as shown in Figures 8 and 9A-9C. Upon receipt of the mating key 822, the CA control system 820 generates one or more EMMs 842 as described above.

[0097] Prior to transmission of the mating key generator 821 and/or Serial Num 841, or elements of these messages are described above, the CA control system 820 may perform an authentication scheme with the mating key gateway 850 in

order to establish a session key to enable secure communications between them.

[0098] Figure 14 is a first exemplary embodiment of the descrambler IC 860 implemented within the digital device 840 of Figure 12. The descrambler IC 860 may be equivalent to construction as descrambler IC 240 of Figures 2, 5 and 7. The descrambler IC 860 comprises at least two process blocks 1010 and 1030 and at least one descrambler unit 1040.

[0099] On receipt of the mating key generator 821 and the encrypted program keys 720_j ($1 \leq j \leq M$), perhaps included in the EMM 842, the first process block 1010 of the descrambler IC 860 performs an encryption or decryption operation on the mating key generator 821 using the Unique Key 880 previously stored in the descrambler IC 860. The encryption or decryption operation may be in accordance with symmetric key cryptographic functions such as DES, AES, IDEA, 3DES and the like. Of course, it is contemplated that the first process block 1010 may be altered to perform a hashing function in lieu of an encryption function.

[00100] The encryption or decryption operation on the mating key generator 821 produces a key 1020 identical to the mating key 822. The key 1020 is loaded into the second process block 1030 and is used to decrypt the encrypted program key 720_j. This recovers the program key used to descramble the scrambled content 848 loaded into the descrambler IC 860. Descrambling may include performance of 3DES or AES operations on the scrambled content. The result may be content in a clear format, which is transmitted from the descrambler IC 860 and subsequently loaded into a MPEG decoder as shown in Figure 5 or optionally into a D/A converter, DVI Interface or IEEE 1394 interface.

[00101] As further shown in Figure 15, an embodiment of the descrambler IC 860 receives a first encrypted program

key ($PK1_{key}$) 1100, the mating key generator 821 and a second encrypted program key 1110 from a second source. The descrambler IC 860 comprises a first process block 1120 that decrypts $PK1_{key}$ 1100 with the Unique Key 880 in accordance with symmetric key cryptographic functions such as AES or 3DES (referred to as "A/3DES") for example.

[00102] The decryption operation on $PK1_{key}$ 1100 recovers a program key 1130, which is loaded into a second process block 1140 that is used to encrypt mating key generator 821 to produce the copy protection key 1150. $PK2_{key}$ 1110 is decrypted by a using the Unique Key 880 (or derivative thereof) to recover the program key in a clear format. The incoming encrypted content 848 is decrypted and/or descrambled within low-level decryption/descrambling logic 1160 of the descrambler IC 860. Decrypting and/or descrambling may include performance of AES or 3DES operations.

[00103] As a result, the content is temporarily placed in a clear format, but is routed to low-level encryption/scrambling logic 1170, which encrypts the descrambled content with the copy protection key 1150 associated with any or all of the destination digital devices. As a result, the content is secure during subsequent transmissions.

[00104] Referring now to Figure 16, a portion of a fifth exemplary embodiment of a secure content delivery system 1200 is shown. In lieu of the subscriber management system 810 and the CA control system 820 of Figure 12, mating key gateway 850 may be adapted for communications with a plurality of subscriber management systems (SMS) 1210_1-1210_K ($K \geq 1$) each associated with a different service provider. Each of these subscriber management systems 1210_1-1210_K supply mating key generators and Serial Nums 1220_1-1220_K to mating key gateway 850 and, in return, receive corresponding mating keys 1230_1-1230_K. These mating keys 1230_1-1230_K are used to encrypt program keys

provided to one or more targeted digital devices (not shown). Alternatively, the trusted third party 435/835 may be utilized as shown in Figures 7, 12 and 16.

[00105] For example, for this illustrated embodiment, subscriber management systems 1210_1 and 1210_2 are terrestrial broadcasters, each providing mating key generators and Serial Nums 1220_1, 1220_2 to mating key gateway 850 and receiving corresponding mating keys 1230_1, 1230_2. Similar in operation, subscriber management systems 1210_3 and 1210_4 are cable operators, subscriber management system 1210_5 is a direct broadcast satellite (DBS) company, and subscriber management systems 1210_{K-1} and 1210_K are Internet content sources.

[00106] In the foregoing description, the invention is described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the present invention as set forth in the appended claims. The specification and drawings are accordingly to be regarded in an illus rather than in a restrictive sense.